Exhibit A

2024 WL 3838423
Only the Westlaw citation is currently available.
United States Court of Appeals, Ninth Circuit.

NETCHOICE, LLC, doing business as NetChoice, Plaintiff - Appellee,

v.

Rob BONTA, Attorney General of the State Of California, Defendant - Appellant.

No. 23-2969
|
Argued and Submitted July 17, 2024 San Francisco, California
|
Filed August 16, 2024

West Codenotes

Validity Called into Doubt
Cal. Civ. Code §§ 1798.99.31(a)(1)-(4), 1798.99.31(c), 1798.99.33, 1798.99.35(c)

Negative Treatment Vacated
Cal. Civ. Code §§ 1798.99.28, 1798.99.29, 1798.99.30, 1798.99.32, 1798.99.40

Appeal from the United States District Court for the Northern District of California Beth Labson Freeman, District Judge, Presiding, D.C. No. 5:22-cv-08861-BLF

Attorneys and Law Firms

Robert Corn-Revere (argued), Foundation for Individual Rights and Expression, Washington, D.C.; David M. Gossett and Meenakshi Krishnan, Davis Wright Tremaine LLP; Washington, D.C.; Ambika Kumar, Davis Wright Tremaine LLP; Seattle, Washington; Adam Sieff, Davis Wright Tremaine LLP; Los Angeles, California; for Plaintiff-Appellee.

Kristin Liska (argued), Deputy Attorney General; Elizabeth Watson, Attorney; Anya Binsacca, Supervising Deputy Attorney General; Thomas S. Patterson, Senior Assistant Attorney General; Rob Bonta, Attorney General of California; Office of the California Attorney General, San Francisco, California; Nicole J. Kau, Deputy Assistant Attorney General, Office of the California Attorney General, Los Angeles, California; for Defendant-Appellant.

John P. Schnapper-Casteras and Rachael Yocum, Schnapper-Casteras PLLC, Washington D.C.; for Amicus Curiae The Institute for Law Innovation and Technology.

Juyoun Han, Patrick K. Lin, and Eric Baum, Eisenberg & Baum LLP, New York, New York; for Amici Curiae Fairplay et al..

Russell C. Bogue, Assistant Attorney General; Ashwin P. Phatak, Principal Deputy Solicitor General; Caroline S. Van Zile, Solicitor General; Brian L. Schwalb, Attorney General for the District of Columbia; Office of the Attorney General for the District of Columbia, Washington, D.C.; Kiel B. Ireland, Deputy Solicitor General; Heidi P. Stern, Solicitor General; Aaron D. Ford, Attorney General for the State of Nevada; Office of the Attorney General for the State of Nevada; for Amici Curiae Nevada, The District of Columbia, Arizona, Arkansas, Colorado, Connecticut, Delaware, Florida, Illinois, Maryland, Michigan, Minnesota, Mississippi, New Jersey, New Mexico, New York, North Carolina, Oregon, Pennsylvania, Rhode Island, and Washington.

Gautam S. Hans, Cornell Law School, Ithaca, New York; for Amici Curiae Privacy and First Amendment Law Professors.

Anne M. Murphy, Joseph W. Cotchett, Karin B. Swope, and Blair Kittle, Cotchett Pitre & McCarthy LLP, Burlingame, California; for Amicus Curiae The American Academy of Pediatrics, The American Psychological Association, and the California Academy of Child and Adolescent Psychiatry.

Marc P. Epstein, Jon Greenbaum, and David Brody, Lawyers' Committee for Civil Rights Under Law, Washington, D.C.; for Amicus Curiae The Lawyers' Committee for Civil Rights Under Law.

Glenn E. Chappell and Hassan A. Zavareei, Tycko & Zavareei LLP, Washington, D.C.; for Amici Curiae Design Scholars.

Jason S. Harrow, Gerstein Harrow LLP, Los Angeles, California; for Amicus Curiae Princeton University Center for Information Technology Policy, Tech Policy Clinic.

Alison S. Gaffney and Dean Kawamoto, Keller Rohrback LLP, Seattle, Washington; for Amici Curiae The American Federation of Teachers and the California Federation of Teachers.

Alvaro M. Bedoya, Commissioner, Federal Trade Commission, Washington, D.C.; for Amicus Curiae Federal Trade Commissioner Alvaro M. Bedoya.

Linda Singer and David I. Ackerman, Motley Rice LLC, Washington, D.C.; for Amici Curiae Elizabeth Denham CBE and Stephan Wood.

Megan Iorio, Tom McBrien, and Suzanne Bernstein, Electronic Privacy Information Center, Washington, D.C.; for Amicus Curiae Electronic Privacy Information Center.

Matthew P. Bergman and Patrick Strekert, Social Media Victims Law Center PLLC, Seattle, Washington; for Amicus Curiae The Center for Humane Technology.

Stephanie A. Joyce, Potomac Law Group PLLC, Washington, D.C.; Computer and Communication Industry Association.

Corbin K. Barthold, TechFreedom, Washington, D.C; for Amicus Curiae TechFreedom.

Megan L. Brown, Kathleen E. Scott, and Boyd Garriott, Wiley Rein LLP, Washington, D.C.; Jonathan D. Urick and Maria C. Monaghan, United States Chamber Litigation Center; Washington, D.C.; for Amicus Curiae Chamber of Commerce of the United States of America.

Brian R. Hardy, Marquis Aurbach Coffing, Las Vegas, Nevada; Ben Sperry and Geoffrey A. Manne; International Center for Law and Economics; Portland, Oregon; for Amicus Curiae International Center for Law and Economics.

Aaron D. Mackey, Adam Schwartz, David Greene, and F. Mario Trujillo, Electronic Frontier Foundation, San Francisco, California; Samir Jain, Eric Null, and Kate Ruane, Center for Democracy and Technology, Washington, D.C.; for Amici Curiae Electronic Frontier Foundation and Center for Democracy and Technology.

Vera Eidelman and Elizabeth Gyori, American Civil Liberties Union Foundation, New York, New York; Jacob A. Snow, Nicolas A. Hidalgo, Chessie Thacher, Nicole A. Ozer, and Matthew T. Cagle, American Civil Liberties Union Foundation of Northern California, San Francisco, California; for Amici Curiae American Civil Liberties Union.

Jessica R. Amunson, Lindsay C. Harrison, and Andrew C. DeGuglielmo, Jenner & Block LLP, Washington, D.C.; for Amicus Curiae Professor Eric Goldman.

Catherine R. Gellis, Sausalito, California; for Amicus Curiae Floor64 Inc., doing business as The Copia Institute.

Mark W. Brennan, J. Ryan Thompson, and Thomas B. Vietch, Hogan Lovells US LLP, Washington, D.C.; Jess Miers, Chamber of Progress, McLean, Virginia; Suzanna Kang, Consumer Technology Association, Arlington, Virginia; Carlos Gutierrez, LGBT Tech, Staunton, Virginia; David Loy, First Amendment Coalition, San Rafael, California; Lawrence Walters, Walters Law Group, Longwood, Florida; for Amici Curiae Chamber of Progress, Consumer Technology Association, First Amendment Coalition, Information Technology and Innovation Foundation, IP Justice, LGBT Tech, The Trevor Project, and Woodhull Freedom Foundation.

Bruce D. Brown, Katie Townsend, Gabe Rottman, Grayson Clary, Emily Hockett, Reporters Committee for Freedom of the Press, Washington, D.C.; for Amici Curiae Reporters Committee for Freedom of the Press and 14 Media Organizations.

Before: MILAN D. SMITH, JR., MARK J. BENNETT, and ANTHONY D. JOHNSTONE, Circuit Judges.

OPINION

M. SMITH, Circuit Judge:

In 2022, the California State Legislature enacted the California Age-Appropriate Design Code Act (CAADCA or Act), Cal. Civ. Code §§ 1798.99.28–1798.99.40, with the express aims of promoting robust online privacy protections for children under the age of eighteen and ensuring that online products that are likely to be accessed by children "are designed in a manner that recognizes the distinct needs of children." *See* 2022 Cal. Legis. Serv. Ch. 320 (A.B. 2273) § 1(b); Cal. Civ. Code § 1798.99.30(b)(1). NetChoice, a national trade association of online businesses with the stated goal of promoting free speech and free enterprise on the Internet, filed suit in the United States District Court for the Northern District of California, challenging the CAADCA on constitutional and federal preemption grounds. The district court found that NetChoice was likely to succeed in its argument that the provisions challenged by NetChoice violated the First Amendment to the U.S. Constitution and were not severable from the valid remainder of the CAADCA. The district court therefore entered a preliminary injunction preventing the entire law from going into effect.

***2** We agree with NetChoice that it is likely to succeed in showing that the CAADCA's requirement that covered businesses opine on and mitigate the risk that children may be exposed to harmful or potentially harmful materials online, Cal. Civ. Code §§ 1798.99.31(a)(1)–(2), facially violates the First Amendment. We therefore affirm the district court's decision to enjoin the enforcement of that requirement, *id.*, and the other provisions that are not grammatically severable from it, *id.* §§ 1798.99.31(a)(3)–(4), (c), 1798.99.33, 1798.99.35(c).

However, we vacate the remainder of the district court's preliminary injunction order, which not only failed to properly consider the facial nature of NetChoice's First Amendment challenges to other provisions of the CAADCA, *id.* §§ 1798.99.31(a)(5)–(7), (9), (b)(1)–(4), (7), but also erroneously overstated the likelihood that NetChoice would ultimately succeed in showing that the unconstitutional portions of the CAADCA are not severable from its valid remainder. We remand to the district court for further proceedings consistent with this opinion.

LEGAL BACKGROUND

In 2018, the California State Legislature enacted the California Consumer Privacy Act (CCPA) to give consumers of all ages "an effective way to control their personal information." 2018 Cal. Legis. Serv. Ch. 55, § 2(i) (A.B. 375). The CCPA requires, among other things, that online providers inform users of the categories of personal information to be collected and the purposes of such collection. *See* Cal. Civ. Code § 1798.100(a)(1). The CCPA applies to "business[es]," defined as for-profit entities that meet certain threshold requirements. *Id.* § 1798.140(d). It further defines "personal information" as any "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." *Id.* § 1798.140(v)(1).

Two years later, in 2020, California voters approved a ballot measure that amended the CCPA to clarify and expand its protections. *See* 2020 Cal. Legis. Serv. Prop. 24. The CCPA, as amended, instructs the California Attorney General to promulgate "regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to ... [s]ubmit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information." Cal Civ. Code § 1798.185(a)(15)(B). The Attorney General ultimately issued a regulation requiring businesses that buy, receive, sell, or share the personal information of 10,000,000 or more consumers in a calendar year to disclose various metrics, including but not limited to the number of requests to delete, to correct, and to know consumers' personal information, as well as the number of requests from consumers to opt out of the sale and sharing of their information. 11 Cal. Code Regs. tit. 11, § 7102(a).

In 2022, the California State Legislature enacted the CAADCA, Cal. Civ. Code §§ 1798.99.28–1798.99.40—the statute which gave rise to this litigation. In its effort to protect the online data privacy of children, defined as consumers under the age of eighteen, *id.* § 1798.99.30(b)(1), the CAADCA imposes several affirmative obligations on "business[es] that provide[ ] an online service, product, or feature likely to be accessed by children," *id.* § 1798.99.31(a).[1] Chief among these mandates is the provision requiring online businesses to create a Data Protection Impact Assessment (DPIA) report identifying, for each offered online service, product, or feature likely to be accessed by children, any risk of "material detriment to children that arise from the data management practices of the business." *Id.* §§ 1798.99.31(a)(1)(A), (B). In creating these DPIA reports, online providers must address the following, to the extent applicable:

> ***3** (i) Whether the design of the online product ... could harm children, including by exposing children to harmful, or potentially harmful, content ....
>
> (ii) Whether the design ... could lead to children experiencing or being targeted by harmful, or potentially harmful, contacts ....
>
> (iii) Whether the design ... could permit children to witness, participate in, or be subject to harmful, or potentially harmful, conduct ....
>
> (iv) Whether the design ... could allow children to be party to or exploited by a harmful, or potentially harmful, contact ....
>
> (v) Whether the algorithms used by the online product ... could harm children.
>
> (vi) Whether targeted advertising systems used by the online product ... could harm children.

> (vii) Whether and how the online product ... uses system design features to increase, sustain, or extend use of the online product ....
>
> (viii) Whether, how, and for what purpose the online product ... collects or processes sensitive personal information of children.

Id. §§ 1798.99.31(a)(1)(B)(i)–(viii). In addition, businesses covered by the CAADCA must "create a timed plan to mitigate or eliminate the risk[s]" identified in a DPIA report "before the online service, product, or feature is accessed by children," *id.* § 1798.99.31(a)(2), and must provide a list of all the DPIA reports the business has completed, or copies of the DPIA reports themselves, to the California Attorney General upon written request, *see id.* §§ 1798.99.31(a)(3), (4).

Apart from the required DPIA reports, the CAADCA also compels online providers to:

> (5) Estimate the age of child users with a reasonable level of certainty appropriate to the risks that arise from the data management practices of the business or apply the privacy and data protections afforded to children to all consumers.
>
> (6) Configure all default privacy settings provided to children by the online service ... to settings that offer a high level of privacy, unless the business can demonstrate a compelling reason that a different setting is in the best interests of children.
>
> (7) Provide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service ....
>
> (8) If the online service, product, or feature allows the child's parent, guardian, or any other consumer to monitor the child's online activity or track the child's location, provide an obvious signal to the child when the child is being monitored or tracked.
>
> ***4** (9) Enforce published terms, policies, and community standards established by the business, including, but not limited to, privacy policies and those concerning children.
>
> (10) Provide prominent, accessible, and responsive tools to help children, or if applicable their parents or guardians, exercise their privacy rights and report concerns.

Id. §§ 1798.99.31(a)(5)–(10).

The CAADCA also forbids "business[es] that provide[ ] an online service, product, or feature likely to be accessed by children," *id.* § 1798.99.31(b), from taking any of the following actions:

> (1) Use the personal information of any child in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child.
>
> (2) Profile a child by default unless ... (A) [t]he business can demonstrate it has appropriate safeguards in place to protect children[ ] [and] (B) [e]ither of the following is true:
>
> > (i) Profiling is necessary to provide the online service ... with which the child is actively and knowingly engaged.
> >
> > (ii) The business can demonstrate a compelling reason that profiling is in the best interests of children.[2]
>
> (3) Collect, sell, share, or retain any personal information that is not necessary to provide [the] online service ... unless the business can demonstrate a compelling reason that [doing so] is in the best interests of children likely to access the online service ....
>
> > (4) If the end user is a child, use personal information for any reason other than a reason for which that personal information was collected, unless the business can demonstrate a compelling reason that use of the personal information is in the best interests of children.
> >
> > (5) Collect, sell, or share any precise geolocation information of children by default unless the collection ... is strictly necessary for the business to provide the service ... requested ....
> >
> > (6) Collect any precise geolocation information of a child without providing an obvious sign to the child for the duration of that collection that precise geolocation information is being collected.
> >
> > (7) Use dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service ... to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being.
> >
> > (8) Use any personal information collected to estimate age or age range for any other purpose or retain that

personal information longer than necessary to estimate age....

Id. §§ 1798.99.31(b)(1)–(8).

The CAADCA exclusively authorizes the California Attorney General to bring a civil enforcement action against any business that fails to comply with the Act's requirements or violates its prohibitions. *See id.* § 1798.99.35(d). Violators are subject to civil penalties of $2,500 per child for each negligent violation and $7,500 for each intentional violation. *See id.* § 1798.99.35(a). However, "[i]f a business is in substantial compliance with" their obligations to create and disclose DPIA reports and to mitigate the risks identified therein, "the Attorney General shall provide written notice to the business, before initiating an [enforcement] action ... identifying the specific provisions of [the CAADCA] that the Attorney General alleges have been or are being violated." *Id.* § 1798.99.35(c)(1). The business then has 90 days to cure the violation before the Attorney General may bring suit. *See id.* § 1798.99.35(c)(2).

***5** The CAADCA also authorizes the creation of a "Children's Data Protection Working Group," comprised of experts in children's data privacy, physical health, mental health and well-being, computer science, and children's rights, and appointed by various members of state government, including the Governor and the Attorney General. *Id.* § 1798.99.32. The working group is tasked with making recommendations to the California State Legislature on "best practices" concerning the data privacy of children, including how children's interests "may be furthered by the design, development, and implementation of an online service, product, or feature" offered by covered business. *Id.* § 1798.99.32(d).

PROCEDURAL HISTORY

NetChoice's members include Amazon, Google, Meta, Netflix, and X. *See About Us*, NetChoice, https://netchoice.org/about/. NetChoice filed this lawsuit against Rob Bonta, the Attorney General of the State of California (the State), on December 14, 2022, challenging the CAADCA as facially unconstitutional and preempted by federal statute. Specifically, the complaint asserts the following claims: (1) violation of the First and Fourteenth Amendments to the U.S. Constitution and Article I, § 2(a) of the California Constitution; (2) violation of the Fourth Amendment to the U.S. Constitution; (3) void for vagueness under the First Amendment and Due Process Clause of the U.S. Constitution and Article I, § 7(a) of the California Constitution; (4) violation of the Commerce Clause of the U.S. Constitution; (5) preemption by the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–06; and (6) preemption by the Communications Decency Act of 1996, specifically, 47 U.S.C. § 230. In particular, NetChoice challenges the mandates of California Civil Code §§ 1798.99.31(a)(1)–(7) and (9), and the prohibitions of subsections (b)(1), (3)–(4), and (7). The complaint requests declaratory and injunctive relief prohibiting enforcement of the CAADCA.

On February 17, 2023, NetChoice moved for a preliminary injunction to enjoin enforcement of the CAADCA, which the district court granted on September 18, 2023. In its order supporting the injunction, the district court began its analysis by observing that "both parties appear to have accepted the relaxed standard for standing in a First Amendment facial challenge," and because of that, the court would consider "arguments about the CAADCA's alleged impact on the expressive activities of individuals and entities who are not NetChoice members." *NetChoice, LLC v. Bonta*, 692 F. Supp. 3d 924, 939 (N.D. Cal. 2023). The district court also stated that it did not need to reach any of NetChoice's First Amendment arguments "based on prior restraint, overbreadth, and vagueness," because NetChoice's arguments about the CAADCA's facial infirmities were "dispositive." *Id.* at 939–40.

The district court then proceeded to analyze whether the CAADCA's provisions implicated protected speech, sufficient to trigger First Amendment scrutiny. In undertaking this threshold inquiry, the district court grouped the CAADCA's provisions into two major categories: its prohibitions, *see* Cal. Civ. Code § 1798.99.31(b), and its affirmative commands, *see id.* § 1798.99.31(a). *NetChoice*, 692 F. Supp. 3d at 942. Regarding the prohibitions, the district court observed that they "forbid the for-profit entities covered by the [CAADCA] from engaging—with some exceptions—in the collection, sale, sharing, or retention of children's personal information, including precise geolocation information, for profiling or other purposes." *Id.* The district court, relying on the Supreme Court's opinion in *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 131 S.Ct. 2653, 180 L.Ed.2d 544 (2011), then concluded that NetChoice is likely to show that the prohibitions necessarily regulate speech protected by the First Amendment because the prohibitions "limit the 'availability and use' of information by certain speakers and for certain purposes," regardless of whether the information

itself constitutes protected speech or is merely a commodity. *NetChoice*, 692 F. Supp. 3d at 944 (quoting *Sorrell*, 564 U.S. at 571, 131 S.Ct. 2653).

***6** As for the CAADCA's affirmative commands, the district court noted that they "are more varied than the [CAADCA's] prohibitions." *Id.* Regarding the DPIA report requirement, the district court held that NetChoice is likely to succeed in showing that the requirement regulates protected speech (and thus triggers First Amendment scrutiny) because the mandatory reports require covered businesses (1) "to express" to the government their "ideas and analysis about likely harm" to children and (2) to take affirmative steps "to mitigate or eliminate the identified risks," for instance, by removing speech that might be harmful to children. *Id.* As for the provisions that require businesses to affirmatively provide information to users, including age-appropriate information about a business's privacy policies, Cal. Civ. Code § 1798.99.31(a)(7), and obvious signals to children if they are being tracked or monitored, *id.* § 1798.99.31(a)(8), the district court found that these sections "necessarily regulate [speech]" as well because they require businesses to engage in speech (thereby triggering the First Amendment). *NetChoice*, 692 F. Supp. 3d at 945.

The district court then analyzed the CAADCA's command that businesses enforce their "published terms, policies, and community standards." Cal Civ. Code § 1798.99.31(a)(9). The district court found that this provision was essentially referring to "content moderation policies." *NetChoice*, 692 F. Supp. 3d at 945. By forcing private businesses to enforce such policies or otherwise face consequences, the district court concluded that CAADCA was necessarily regulating speech protected by the First Amendment.[3] *Id.* As for the two sections of the CAADCA requiring businesses to estimate the age of child users and provide them with a high default privacy setting or forego age estimation and provide a high default privacy setting to all users, Cal Civ. Code §§ 1798.99.31(a)(5)–(6), the district court found that "the steps a business would need to take to sufficiently estimate the age of child users would likely prevent both children and adults from accessing certain content." *NetChoice*, 692 F. Supp. 3d at 945. Because these provisions would likely "impede the 'availability and use' of information," the district court concluded that they triggered First Amendment scrutiny as well. *Id.* at 946 (quoting *Sorrell*, 564 U.S. at 571, 131 S.Ct. 2653). Considering all the above, the district court held "that NetChoice is likely to succeed in showing that the CAADCA's prohibitions and mandates regulate speech, so that the Act triggers First Amendment scrutiny." *Id.*

Next, to determine the appropriate level of judicial scrutiny, the district court examined what types of speech are implicated by the CAADCA—i.e., commercial or non-commercial speech. *Id.* The district court ultimately found that it was "difficult to determine whether the [CAADCA] regulates only commercial speech." *Id.* at 947. Accordingly, the court assumed for the purposes of the motion for a preliminary injunction "that only the lesser standard of intermediate scrutiny for commercial speech applies" because the outcome of the analysis would be the same under both intermediate scrutiny and strict scrutiny. *Id.* at 948.

Applying "commercial speech scrutiny," [4] the district court first determined that "the CAADCA regulates speech that is neither misleading nor related to unlawful activity." *Id.* Next, the court found that NetChoice was unlikely to show that California failed to substantiate its substantial interest in protecting the physical, mental, and emotional health and well-being of minors online. *Id.* at 948–49. Therefore, the district court proceeded to examine whether the CAADCA "directly advance[s] the state interest involved," and whether it is not "more extensive than is necessary to serve that interest." *Id.* at 948 (quoting *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 566, 100 S.Ct. 2343, 65 L.Ed.2d 341 (1980)). The district court ultimately agreed with NetChoice that it was likely to show that all of the provisions it challenged— §§ 1798.99.31(a)(1)–(7), 1798.99.31(a)(9), 1798.99.31(b)(1)–(4), and 1798.99.31(b)(7)—failed *Central Hudson*'s means-ends inquiry.[5] *NetChoice*, 692 F. Supp. 3d at 949–59.

***7** The district court then examined whether it could sever the unconstitutional provisions from the remainder of the statute and concluded that it could not, primarily because of the unconstitutional DPIA report requirement. *Id.* at 960. Specifically, if a business is in substantial compliance with its obligation to create, disclose, and mitigate the risks identified in its regular DPIA reports, the Attorney General must give it written notice of possible violations and an opportunity to cure them before bringing suit. *See* Cal. Civ. Code §§ 1798.99.35(c)(1), (2). The district court concluded that, without the DPIA reports, it was impossible to enforce any of the other valid provisions of the CAADCA in the manner in which the California Legislature had envisioned. *NetChoice*, 692 F. Supp. 3d at 960. While the district court found that the inability to sever the DPIA provisions was

wholly determinative of the issue, the court also outlined other reasons why attempting to sever other unconstitutional provisions from the statute would be unworkable or futile. *Id.* at 960–61.

The court declined to issue preliminary rulings on the merits of NetChoice's remaining claims, since it was clear to the court that NetChoice was likely to succeed on its facial claim brought under the First Amendment. *Id.* at 961–64. Upon concluding that NetChoice met the remaining preliminary injunction factors under *Winter v. Natural Resources Defense Council, Inc.*, 555 U.S. 7, 129 S.Ct. 365, 172 L.Ed.2d 249 (2008), on that claim, the court enjoined enforcement of the CAADCA in its entirety. *NetChoice*, 692 F. Supp. 3d at 964–65. The State timely appealed.

JURISDICTION AND STANDARD OF REVIEW

We have jurisdiction pursuant to 28 U.S.C. § 1292(a)(1) to review the district court's grant of a preliminary injunction. *Daniels Sharpsmart, Inc. v. Smith*, 889 F.3d 608, 613 (9th Cir. 2018). "We review the district court's decision to grant a preliminary injunction for abuse of discretion." *Id.* "A district court abuses its discretion if it rests its decision 'on an erroneous legal standard or on clearly erroneous factual findings.' " *Am. Beverage Ass'n v. City & Cnty. of San Francisco*, 916 F.3d 749, 754 (9th Cir. 2019) (en banc) (quoting *United States v. Schiff*, 379 F.3d 621, 625 (9th Cir. 2004)). "A district court's decision is based on an erroneous legal standard if: '(1) the court did not employ the appropriate legal standards that govern the issuance of a preliminary injunction; or (2) in applying the appropriate standards, the court misapprehended the law with respect to the underlying issues in the litigation.' " *Cal. Chamber of Com. v. Council for Educ. & Rsch. on Toxics*, 29 F.4th 468, 475 (9th Cir. 2022) (quoting *Negrete v. Allianz Life Ins. Co. of N. Am.*, 523 F.3d 1091, 1096 (9th Cir. 2008)), *cert. denied*, —— U.S. ——, 143 S. Ct. 1749, 215 L.Ed.2d 649 (2023).

ANALYSIS

"A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter*, 555 U.S. at 20, 129 S.Ct. 365. On appeal, the State does not meaningfully contest the district court's determinations regarding the balance of equities, irreparable injury, and public interest factors, but does insist that NetChoice is not likely to succeed on the merits of its First Amendment challenge to the CAADCA. Accordingly, our analysis focuses on whether NetChoice is likely to succeed on the merits of its First Amendment challenge.

I. NetChoice Is Likely to Succeed in Showing That the DPIA Report Requirement Facially Violates the First Amendment.

"For a host of good reasons, courts usually handle constitutional claims case by case, not en masse." *Moody*, 144 S. Ct. at 2397. The Supreme Court "has therefore made facial challenges hard to win." *Id.* In a typical facial challenge, "a plaintiff cannot succeed unless he 'establish[es] that no set of circumstances exists under which the [law] would be valid,' or he shows that the law lacks a 'plainly legitimate sweep.' " *Id.* (alterations in original) (first quoting *United States v. Salerno*, 481 U.S. 739, 745, 107 S.Ct. 2095, 95 L.Ed.2d 697 (1987); and then quoting *Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 449, 128 S.Ct. 1184, 170 L.Ed.2d 151 (2008)).

***8** However, in First Amendment cases, the Supreme Court "has lowered that very high bar." *Id.* "To provide breathing room for free expression," the Supreme Court has "substituted a less demanding though still rigorous standard." [6] *Id.* (cleaned up); *see also Tucson v. City of Seattle*, 91 F.4th 1318, 1327 (9th Cir. 2024). "[I]f the law's unconstitutional applications substantially outweigh its constitutional ones," then a court may sustain a facial challenge to the law and strike it down. *Moody*, 144 S. Ct. at 2397. As *Moody* clarified, a First Amendment facial challenge has two parts: first, the courts must "assess the state laws' scope"; and second, the courts must "decide which of the laws' applications violate the First Amendment, and ... measure them against the rest." *Id.* at 2398.

Just like the parties and lower courts in *Moody*, "no one has paid much attention to" the requirements for a facial challenge so far in this case. *Id.* Nevertheless, for the reasons set forth immediately below, we conclude that this oversight did not cause any error in the district court's analysis of the CAADCA's DPIA report requirement. *See* Cal. Civ. Code §§ 1798.99.31(a)(1)–(2). That is because the DPIA report requirement, in every application to a covered business, raises the same First Amendment issues.

Specifically, every business covered by the CAADCA must create DPIA reports identifying, for each offered online service, product, or feature likely to be accessed by children, any risk of "material detriment to children that arise from the data management practices of the business." Cal. Civ. Code §§ 1798.99.31(a)(1)(A), (B). In creating those reports, every covered business must assess eight different factors related to "harm" prior to offering a new online service, product, or feature that is likely to be accessed by children. *See id.* These factors include whether the design of the product may expose children to harmful or potentially harmful content and whether it may permit children to witness harmful, or potentially harmful, conduct. *Id.* §§ 1798.99.31(a)(1)(B)(i), (iii). Covered businesses are then required to "[d]ocument any risk of material detriment to children that arises from the data management practices of the business identified in the" DPIA required in § 1798.99.31(a)(1), including the eight enumerated factors. *Id.* § 1798.99.31(a)(2). Once these risks are identified, every covered business must then "create a timed plan to mitigate or eliminate the risk [of material detriment to children] before the online service, product, or feature is accessed by children." *Id.*

Whether it be NetChoice's members or other covered businesses providing online services likely to be accessed by children, all of them are under the same statutory obligation to opine on and mitigate the risk that children may be exposed to harmful or potentially harmful content, contact, or conduct online. While it is certainly possible that in some applications, a covered business will ultimately conclude that it need not address certain risks in its DPIA report because its new service to be offered does not create such risks, *see id.* § 1798.99.31(a)(1)(B) (stating that a covered business shall address the eight factors "to the extent applicable"), there is no question that a covered business at the threshold would still have to inquire into whether the risk exists before it can decline to address it in its DPIA report. Therefore, in every circumstance in which a covered business creates a DPIA report for a particular service, the business must ask whether the new service may lead to children viewing or receiving harmful or potentially harmful materials. Whether the State can impose such a requirement without running afoul of the First Amendment may be answered without speculation "about 'hypothetical' or 'imaginary' cases." *Wash. State Grange*, 552 U.S. at 450, 128 S.Ct. 1184.

***9** Accordingly, unlike the record in the *Moody* case, the record here is sufficiently developed to consider the scope of the DPIA provision and whether its unconstitutional applications substantially outweigh its constitutional ones. We therefore proceed to consider whether the requirement is likely to survive NetChoice's First Amendment facial challenge.

A. The DPIA Report Requirement Undoubtedly Regulates Protected Speech, Thereby Implicating the First Amendment.

The State argues that the DPIA report requirement is "incidental to [the CAADCA's] legitimate goals of protecting children from excessive data collection and use and thus is not subject to heightened [First Amendment] scrutiny." The State further contends that the role of the DPIA report requirement is simply "to incentivize businesses to be proactive about their management of children's data by offering businesses that complete the DPIA a 90-day period to cure violations of the Act without penalty," and does "not compel businesses to express a message or interfere with any message a business might wish to send."

In response, NetChoice argues that the DPIA report requirement "constructs a censorship regime," and "compels services to speak," and therefore, invites First Amendment scrutiny. According to NetChoice, the DPIA report requirement has little to do with privacy and instead "force[s] covered businesses to identify and disclose to the government potential risks that minors might be exposed to potentially harmful *content* [online] and [to] develop a timed plan to mitigate or eliminate the identified risks before publication" (cleaned up).

We agree with NetChoice that the DPIA report requirement, codified at §§ 1798.99.31(a)(1)–(2) of the California Civil Code, triggers review under the First Amendment. First, the DPIA report requirement clearly compels speech by requiring covered businesses to opine on potential harm to children. It is well-established that the First Amendment protects "the right to refrain from speaking at all." *Wooley v. Maynard*, 430 U.S. 705, 714, 97 S.Ct. 1428, 51 L.Ed.2d 752 (1977); *see also 303 Creative LLC v. Elenis*, 600 U.S. 570, 586, 143 S.Ct. 2298, 216 L.Ed.2d 1131 (2023). It is also well-established that the forced disclosure of information, even purely commercial information, triggers First Amendment scrutiny. *See Zauderer v. Off. of Disciplinary Counsel of Sup. Ct. of Ohio*, 471 U.S. 626, 629, 650–53, 105 S.Ct. 2265, 85 L.Ed.2d 652 (1985) (applying First Amendment scrutiny to a law that required attorneys to disclose in their advertising certain information regarding fee arrangements); *Nat'l Ass'n of Wheat Growers v.*

Bonta, 85 F.4th 1263, 1266, 1275 (9th Cir. 2023) (applying First Amendment scrutiny to a law requiring businesses to warn consumers that glyphosate is a carcinogen); *see also Sorrell*, 564 U.S. at 570, 131 S.Ct. 2653 ("This Court has held that the creation and dissemination of information are speech within the meaning of the First Amendment."). Nor can we, as the State suggests, ignore that the DPIA requirement compels speech simply because other parts of the CAADCA may primarily or exclusively regulate non-expressive conduct. The primary effect of the DPIA provision is to compel speech, distinguishing it from statutes where the compelled speech was "plainly incidental to the [law's] regulation of conduct." *Rumsfeld v. Forum for Acad. & Inst. Rights, Inc.*, 547 U.S. 47, 62, 126 S.Ct. 1297, 164 L.Ed.2d 156 (2006); *see also Sorrell*, 564 U.S. at 567, 131 S.Ct. 2653 (providing examples of conduct regulations that have incidental burdens on speech). The State cannot insulate a specific provision of law from a facial challenge under the First Amendment by bundling it with other, separate provisions that do not implicate the First Amendment.

***10** The State makes much of the fact that the DPIA reports are not public documents and retain their confidential and privileged status even after being disclosed to the State, but the State provides no authority to explain why that fact would render the First Amendment wholly inapplicable to the requirement that businesses create them in the first place. On the contrary, the Supreme Court has recognized the First Amendment may apply even when the compelled speech need only be disclosed to the government. *See Ams. for Prosperity Found. v. Bonta*, 594 U.S. 595, 616, 141 S.Ct. 2373, 210 L.Ed.2d 716 (2021). Accordingly, the district court did not err in concluding that the DPIA report requirement triggers First Amendment scrutiny because it compels protected speech.

Second, the DPIA report requirement invites First Amendment scrutiny because it deputizes covered businesses into serving as censors for the State. The Supreme Court has previously applied First Amendment scrutiny to laws that deputize private actors into determining whether material is suitable for kids. *See Interstate Cir., Inc. v. City of Dallas*, 390 U.S. 676, 678, 684, 88 S.Ct. 1298, 20 L.Ed.2d 225 (1968) (recognizing that a film exhibitor's First Amendment rights were implicated by a law requiring it to inform the government whether films were "suitable" for children). Moreover, the Supreme Court recently affirmed "that laws curtailing [ ] editorial choices [by online platforms] must meet the First Amendment's requirements." *Moody*, 144 S. Ct. at 2393.

The State resists NetChoice's characterization of the DPIA report requirement as constructing a censorship scheme by arguing that "the mitigation requirement contains *no* reference to content whatsoever; it solely requires a company to mitigate risks from its *data management practices*." But that argument ignores that § 1798.99.31(a)(2) specifically defines data management practices by reference to the statutory factors a covered business must assess under § 1798.99.31(a)(1)(B) when assessing those risks. Those factors require consideration of content or proxies for content. For instance, the CAADCA expressly requires a covered business to assess "[w]hether the design of the online product ... could ... expos[e] children to harmful, or potentially harmful, content on the online product"; "[w]hether the design ... could lead to children experiencing or being targeted by harmful, or potentially harmful, contacts"; and "[w]hether the design ... could permit children to witness, participate in, or be subject to harmful, or potentially harmful, conduct." Cal. Civ. Code §§ 1798.99.31(a)(1)(B)(i)–(iii). The CAADCA unquestionably requires a covered business to mitigate that risk, and the State's argument to the contrary has failed to convince us otherwise.

At oral argument, the State suggested companies could analyze the risk that children would be exposed to harmful or potentially harmful material without opining on what material is potentially harmful to children. However, a business cannot assess the likelihood that a child will be exposed to harmful or potentially harmful materials on its platform without first determining what constitutes harmful or potentially harmful material. To take the State's own example, data profiling may cause a student who conducts research for a school project about eating disorders to see additional content about eating disorders. Unless the business assesses whether that additional content is "harmful or potentially harmful" to children (and thus opines on what sort of eating disorder content is harmful), it cannot determine whether that additional content poses a "risk of material detriment to children" under the CAADCA. Nor can a business take steps to "mitigate" the risk that children will view harmful or potentially harmful content if it has not identified what content should be blocked.

***11** Accordingly, the district court was correct to conclude that the CAADCA's DPIA report requirement regulates the speech of covered businesses and thus triggers review under the First Amendment.

B. Strict Scrutiny Applies to the DPIA Report Requirement.

Given that the DPIA report requirement triggers review under the First Amendment, the district court then needed to determine the appropriate level of scrutiny in assessing whether NetChoice was likely to succeed in showing that the requirement violates the First Amendment. In its preliminary injunction order, the district court found that it was "difficult to determine whether the [CAADCA] regulates only commercial speech." *NetChoice*, 692 F. Supp. 3d at 947. Accordingly, the court assumed for the purposes of the preliminary injunction "that only the lesser standard of intermediate scrutiny for commercial speech applies" because the outcome of the analysis would be the same under both intermediate commercial speech scrutiny and strict scrutiny. *Id.* at 947–48. While we understand the district court's caution against prejudicing the merits of the case at the preliminary injunction stage, there is no question that strict scrutiny, as opposed to mere commercial speech scrutiny, governs our review of the DPIA report requirement.

Laws regulating commercial speech are generally subject to a lesser standard than strict scrutiny. *See Cent. Hudson*, 447 U.S. at 563–66, 100 S.Ct. 2343. Speech is commercial when it "does 'no more than propose a commercial transaction.' " *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 66, 103 S.Ct. 2875, 77 L.Ed.2d 469 (1983) (quoting *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 762, 96 S.Ct. 1817, 48 L.Ed.2d 346 (1976)). We have recognized that the "commercial speech 'analysis is fact-driven, due to the inherent "difficulty of drawing bright lines that will clearly cabin commercial speech in a distinct category." ' " *First Resort, Inc. v. Herrera*, 860 F.3d 1263, 1272 (9th Cir. 2017) (quoting *Greater Balt. Ctr. for Pregnancy Concerns, Inc. v. Mayor & City Council of Balt.*, 721 F.3d 264, 284 (4th Cir. 2013)). Therefore, in close cases, we consider the three factors identified by the Supreme Court in *Bolger v. Youngs Drug Products Corporation*, to determine if speech is commercial. *Id.* (" '[S]trong support' that the speech should be characterized as commercial speech is found where the speech is an advertisement, the speech refers to a particular product, and the speaker has an economic motivation." (quoting *Hunt v. City of Los Angeles*, 638 F.3d 703, 715 (9th Cir. 2011))). If commercial speech is misleading or related to illegal activity, it is not entitled to protection. *Cent. Hudson*, 447 U.S. at 563–64, 100 S.Ct. 2343. As for laws that compel the disclosure of "purely factual and uncontroversial" commercial speech, such laws are subject to a form of rational basis review. *Zauderer*, 471 U.S. at 651, 105 S.Ct. 2265. For all other commercial speech, courts must apply a form of intermediate scrutiny by asking "whether the asserted governmental interest is substantial," "whether the regulation directly advances the governmental interest asserted," and "whether [the law] is not more extensive than is necessary to serve that interest." *Cent. Hudson*, 447 U.S. at 566, 100 S.Ct. 2343.

***12** The DPIA report requirement—in requiring covered businesses to opine on and mitigate the risk that children are exposed to harmful content online—regulates far more than mere commercial speech. In the DPIA report, a covered business must do far "more than propose a commercial transaction." *Va. State Bd. of Pharmacy*, 425 U.S. at 762, 96 S.Ct. 1817. Instead, businesses covered by the CAADCA must opine on potential speech-based harms to children, including harms resulting from the speech of third parties, disconnected from any economic transaction. *Cf. Riley v. Nat'l Fed'n of the Blind of N.C., Inc.*, 487 U.S. 781, 796, 108 S.Ct. 2667, 101 L.Ed.2d 669 (1988) ("Our lodestars in deciding what level of scrutiny to apply to a compelled statement must be the nature of the speech taken as a whole and the effect of the compelled statement thereon."); *Wheat Growers*, 85 F.4th at 1266, 1275 (assuming that a warning to customers about a carcinogen is purely commercial speech). The mere fact that a business may earn revenue from its services is "insufficient by itself" to render its opinions about those services "commercial." *Bolger*, 463 U.S. at 67, 103 S.Ct. 2875. And the DPIA requirement goes further, because it not only requires businesses to identify harmful or potentially harmful content but also requires businesses to take steps to protect children from such content. Therefore, the DPIA report requirement appears to meet none of the three *Bolger* factors: (1) the reports are not advertisements, (2) they require businesses to go beyond opining about their products or services to opine on highly controversial issues of public concern and then take steps to censor material that the company has deemed sufficiently harmful, and (3) businesses do not have a clear economic motivation to provide these opinions or perform this state-required censorship. The same can be said for the speech that businesses are deputized into self-censoring by operation of the CAADCA's mitigation provision. There should be no doubt that the speech children might encounter online while using covered businesses' services is not mere commercial speech. Further, a business's opinion about how its services might expose children to harmful content online is not "purely factual and uncontroversial." *Zauderer*, 471 U.S. at 651, 105 S.Ct. 2265. We therefore conclude that the subjective

opinions compelled by the CAADCA are best classified as non-commercial speech. *See Riley*, 487 U.S. at 796, 108 S.Ct. 2667 ("[W]e do not believe that the speech retains its commercial character when it is inextricably intertwined with otherwise fully protected speech.").

Amicus Institute for Law, Innovation & Technology (iLIT) contends that the district court "fundamentally misunderst[oo]d what DPIAs entail, how they are used, where they originated, when they are necessary—and the central fact that they are widespread and commonly used." Tellingly, iLit compares the CAADCA's DPIA report requirement with a supposedly "similar DPIA requirement" found in the CCPA, and proceeds to argue that the district court's striking down of the DPIA report requirement in the CAADCA necessarily threatens the same requirement in the CCPA. But a plain reading of the relevant provisions of both laws reveals that they are not the same; indeed, they are vastly different in kind.

Under the CCPA, businesses that buy, receive, sell, or share the personal information of 10,000,000 or more consumers in a calendar year are required to disclose various metrics, including but not limited to the number of requests to delete, to correct, and to know consumers' personal information, as well as the number of requests from consumers to opt out of the sale and sharing of their information. 11 Cal. Code Regs. tit. 11, § 7102(a); *see* Cal Civ. Code § 1798.185(a)(15)(B) (requiring businesses to conduct regular risk assessments regarding how they process "sensitive personal information"). That obligation to collect, retain, and disclose purely factual information about the number of privacy-related requests is a far cry from the CAADCA's vague and onerous requirement that covered businesses opine on whether their services risk "material detriment to children" with a particular focus on whether they may result in children witnessing harmful or potentially harmful content online. A DPIA report requirement that compels businesses to measure and disclose to the government certain types of risks potentially created by their services might not create a problem. The problem here is that the risk that businesses must measure and disclose to the government is the risk that children will be exposed to disfavored speech online. Accordingly, iLIT's concern that the district court's ruling necessarily threatens other DPIA schemes throughout the country, is misguided.

Considering the above, the district court in its preliminary injunction analysis should have subjected the DPIA report requirement to strict scrutiny, as opposed to mere intermediate commercial scrutiny. Strict scrutiny is warranted because the DPIA report requirement (1) compels speech with a particular message about controversial issues, *see Nat'l Inst. of Fam. & Life Advocs. v. Becerra*, 585 U.S. 755, 766, 138 S.Ct. 2361, 201 L.Ed.2d 835 (2018); and (2) deputizes private actors into censoring speech based on its content, *see United States v. Playboy Ent. Grp., Inc.*, 529 U.S. 803, 806, 813, 120 S.Ct. 1878, 146 L.Ed.2d 865 (2000). While it is true that "a State possesses legitimate power to protect children from harm, [ ] that does not include a free-floating power to restrict the ideas to which children may be exposed." *Brown v. Ent. Merchants Ass'n*, 564 U.S. 786, 794, 131 S.Ct. 2729, 180 L.Ed.2d 708 (2011) (citations omitted).

C. The DPIA Report Requirement Likely Fails Strict Scrutiny.

***13** Although the district court stopped short of concluding that strict scrutiny governed its review of the DPIA report requirement, the court's ultimate conclusion that the DPIA report requirement is likely to fail First Amendment scrutiny was correct.

Assuming arguendo that the State has a compelling interest in protecting children from "being pushed ... unwanted material, such as videos promoting self-harm," as the State itself contends, the State is unlikely to show that the DPIA report requirement is "the least restrictive means" available for advancing that interest. *Playboy Ent. Grp.*, 529 U.S. at 813, 120 S.Ct. 1878. As Amici American Civil Liberties Union and American Civil Liberties Union of Northern California (together, the ACLU) note in their amicus brief, the CAADCA's broad requirement that companies identify the risk of children being exposed to potentially harmful content necessarily compels companies to "assess the potential for [online] material to instigate grief, sorrow, pain, hurt, distress, or affliction in a minor." Such material

> includes online mental health resources and communities that many children turn to for support. It touches reporting about school shootings, war, climate change, and teen suicide. And it reaches minors' own political or religious speech, as well as their personal updates about deaths in the family, rejection from a college, or a breakup.

The State could have easily employed less restrictive means to accomplish its protective goals, such as by (1) incentivizing companies to offer voluntary content filters or application blockers, (2) educating children and parents on the importance of using such tools, and (3) relying on existing criminal laws that prohibit related unlawful conduct.

The State also asserts that the DPIA report requirement protects children's safety by encouraging companies to proactively assess "how their products use children's data and whether their data management practices or product designs pose risks to children," so that "fewer children will be subject to preventable harms." Again, assuming this interest is compelling, the DPIA report requirement is still likely to fail on the tailoring-end of the analysis. *See Playboy*, 529 U.S. at 813, 120 S.Ct. 1878. While it is true that some of the specific factors businesses are required to assess in their DPIA reports are directly related to remedying harms arising from a business's data management practices and design features, *see* Cal Civ. Code §§ 1798.99.31(a)(1)(B)(vii), (viii) (requiring self-assessments about harmful design features and data collection practices), the relevant provisions are worded at such a high level of generality that they provide little help to businesses in identifying which of those practices or designs may actually harm children. Nor does the presence of these factors overcome the fact that most of the factors the State requires businesses to assess in their DPIA reports compel them to guard against the risk that children may come across potentially harmful content while using their services, *see id.* §§ 31(a)(1)(B)(i), (ii), (iii), (iv), (vi), which is hardly evidence of narrow tailoring.[7]

***14** In addition, a disclosure regime that requires the forced creation and disclosure of highly subjective opinions about content-related harms to children is unnecessary for fostering a proactive environment in which companies, the State, and the general public work to protect children's safety online. For instance, the State could have developed a disclosure regime that defined data management practices and product designs without reference to whether children would be exposed to harmful or potentially harmful content or proxies for content. Instead, the State attempts to indirectly censor the material available to children online, by delegating the controversial question of what content may "harm to children" to the companies themselves, thereby raising further questions about the onerous DPIA report requirement's efficacy in achieving its goals. And while the State may be correct the DPIA reports' confidentiality reflect a degree of narrow tailoring by minimizing the burden of forcing businesses to speak on controversial issues, that feature may also cut against the DPIA report requirement's effectiveness at informing the greater public about how covered businesses use and exploit children's data.

Ultimately, the DPIA report requirement falls well short of satisfying strict First Amendment scrutiny. The district court was therefore correct to conclude that NetChoice is likely to succeed in showing that the DPIA report requirement facially violates the First Amendment.

II. It Is Unclear From the Record Below Whether Other Challenged Provisions of the CAADCA Facially Violate the First Amendment.

In every application of the DPIA report requirement to a covered business, the DPIA report requirement raises the same First Amendment issues. Accordingly, the current record allows us to analyze whether the DPIA report requirement is likely to violate the First Amendment was through a facial challenge. Whether NetChoice is likely to succeed on its facial challenge as to the remaining provisions it challenges is less certain. For instance, most of those provisions, by their plain language, do not necessarily impact protected speech in all or even most applications. *See* Cal. Civ. Code §§ 1798.99.31(a)(5)–(6), (9), (b)(1)–(4), (7). As in *Moody*, the record needs further development to allow the district court to determine "the full range of activities the law[ ] cover[s]." *Moody*, 144 S. Ct. at 2397. But even for the remaining provision that is likely to trigger First Amendment scrutiny in every application because the plain language of the provision compels speech by covered businesses, *see* Cal. Civ. Code §§ 1798.99.31(a)(7), we cannot say, on this record, that a substantial majority of its applications are likely to fail First Amendment scrutiny.

Consider, for instance, the CAADCA's prohibition against using

> dark patterns to lead or encourage children to provide personal information beyond what is reasonably expected to provide that online service ... to forego privacy protections, or to take any action that the business knows, or has reason to know, is materially detrimental to the child's physical health, mental health, or well-being.

Cal. Civ. Code § 1798.99.31(b)(7). California law defines a "dark pattern" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice." *Id.* § 1798.140(l). Based on the record developed so far in this litigation, it is unclear whether a "dark pattern" itself constitutes protected speech and whether a ban on using "dark patterns" should always trigger First Amendment scrutiny, and the district court never grappled with this question.[8] Moreover, even in applications where the ban on "dark patterns" is likely

to impact other categories of protected speech, such as the editorial decisions of social media companies, it is far from certain that such a ban should be scrutinized as a content-based restriction, as opposed to a content-neutral regulation of expression. *See United States v. O'Brien*, 391 U.S. 367, 376–77, 88 S.Ct. 1673, 20 L.Ed.2d 672 (1968). Without considering the full range of how the CAADCA's ban on "dark patterns" might apply to covered businesses, the district court had no basis to conclude that NetChoice was likely to succeed in its facial challenge to the ban. *See Moody*, 144 S. Ct. at 2397–98.

***15** The district court also sustained facial attacks on several other provisions that, on their face, do not necessarily impact protected speech in all or even most applications. *See* Cal. Civ. Code §§ 1798.99.31(a)(1)(5)–(6), (9), (b)(1)–(4). Notably, the district court concluded that many of these provisions were unlikely to survive First Amendment scrutiny because of its finding that these requirements would ultimately curtail the editorial decisions of social media companies covered by the CAADCA or chill the expression of their third-party users. But the focus on whether and how these provisions may impact content moderation policies, without considering any other potential applications, treats NetChoice's challenges "more like as-applied claims than like facial ones." *Moody*, 144 S. Ct. at 2398. Instead, the court focused on possible applications of these provisions to social media companies —a subset of the businesses covered by the CAADCA— and speculated about how that subset of applications could ultimately have a substantial effect on those companies' editorial discretion or the expression of their third-party users.

The only remaining provision challenged by NetChoice that clearly triggers First Amendment scrutiny in all its applications is § 1798.99.31(a)(7) of the CAADCA, which requires online businesses to "[p]rovide any privacy information, terms of service, policies, and community standards concisely, prominently, and using clear language suited to the age of children likely to access that online service, product, or feature." In every application of that provision to a covered business, it compels speech and triggers First Amendment scrutiny. However, it is unclear from the record below whether a substantial majority of those applications are likely to fail First Amendment scrutiny. In many circumstances, all or most of the speech compelled by this provision is likely to be purely factual and non-controversial. *See Zauderer*, 471 U.S. at 651, 105 S.Ct. 2265. However, the district court never explored that possibility because it assumed that this provision primarily dealt with social media companies' disclosure of content-moderation policies and that such disclosures were subject to strict scrutiny. *NetChoice*, 692 F. Supp. 3d at 945, 953–54.

In light of the above, we conclude that the district court's failure to properly consider the facial nature of NetChoice's challenges to §§ 1798.99.31(a)(5)–(7), (9), (b)(1)–(4), (7) of the CAADCA makes it practically impossible for us to determine on appeal whether these provisions are likely to facially violate the First Amendment. That failure alone is enough for us to vacate the district court's preliminary injunction as to those provisions. *See Sports Form, Inc. v. United Press Int'l, Inc.*, 686 F.2d 750, 752 (9th Cir. 1982) ("A district court's order [granting or denying a preliminary injunction] is reversible for legal error if the court ... misapprehends the law with respect to the underlying issues in litigation.").

III. It Is Too Early to Determine Whether the Unconstitutional Provisions of the CAADCA Are Likely Severable from Its Valid Remainder.

Because it is unclear to us whether NetChoice is likely to succeed in its facial challenges to §§ 1798.99.31(a)(5)–(7), (9), (b)(1)–(4), (7) of the CAADCA, it is premature for us to consider as a whole whether the invalid portions of the CAADCA are severable from the valid remainder of the statute. *See Calfarm Ins. Co. v. Deukmejian*, 48 Cal.3d 805, 258 Cal.Rptr. 161, 771 P.2d 1247, 1255–56 (1989). We do not have a full picture of what the invalid portions of the CAADCA are likely to be. Nevertheless, we do have enough information from the record below to review the district court's determination that the DPIA report requirement, *see* Cal. Civ. Code §§ 1798.99.31(a)(1)–(2), is unlikely to be severable from provisions of the law that NetChoice does not challenge on First Amendment grounds, *see, e.g.*, *id.* §§ 1798.99.32, 1798.99.35.

"Severability is ... a matter of state law." *Sam Francis Found. v. Christies, Inc.*, 784 F.3d 1320, 1325 (9th Cir. 2015) (alteration in original) (quoting *Leavitt v. Jane L.*, 518 U.S. 137, 139, 116 S.Ct. 2068, 135 L.Ed.2d 443 (1996)). "In California, the presence of a severability clause in a statutory scheme that contains an invalid provision 'normally calls for sustaining the valid part of the enactment.' " *Garcia v. City of Los Angeles*, 11 F.4th 1113, 1120 (9th Cir. 2021) (quoting *Cal. Redevelopment Ass'n v. Matosantos*, 53 Cal.4th 231, 135 Cal.Rptr.3d 683, 267 P.3d 580, 607 (2011)). No such severability clause exists in the CAADCA.

***16** Regardless of whether there is a severability clause, courts must also examine whether the invalid portion of a statute is "grammatically, functionally, and volitionally" severable from the valid remainder of the statute. *Calfarm Ins. Co.*, 258 Cal.Rptr. 161, 771 P.2d at 1256; *Legislature v. Eu*, 54 Cal.3d 492, 286 Cal.Rptr. 283, 816 P.2d 1309, 1335 (1991) ("[I]t is clear that severance of particular provisions is permissible despite the absence of a formal severance clause."). A provision is "grammatically" severable "if it is 'distinct' and 'separate' and, hence, 'can be removed as a whole without affecting the wording of any' of the measure's other provisions.' " *Hotel Emps. & Rest. Emps. Int'l Union v. Davis*, 21 Cal.4th 585, 88 Cal.Rptr.2d 56, 981 P.2d 990, 1009 (1999) (quoting *CalFarm Ins. Co.*, 258 Cal.Rptr. 161, 771 P.2d at 1256). An invalid part of a law is "functionally" severable "if it is not necessary to the measure's operation and purpose." *Id.* In other words, the "part to be severed must not be part of a partially invalid but unitary whole. The remaining provisions must stand on their own, unaided by the invalid provisions nor rendered vague by their absence nor inextricably connected to them by policy considerations. They must be capable of separate enforcement." *People's Advoc., Inc. v. Superior Ct.*, 181 Cal.App.3d 316, 226 Cal. Rptr. 640, 649 (1986). Volitional severability "depends on whether the remainder would have been adopted by the legislative body had the latter foreseen the partial invalidation of the statute." *Matosantos*, 135 Cal.Rptr.3d 683, 267 P.3d at 608 (internal quotation marks omitted).

Here, §§ 1798.99.31(a)(3)–(4), (c), 1798.99.33, 1798.99.35(c) of the CAADCA all explicitly refer to the DPIA report requirement. Without the DPIA report requirement, these remaining provisions no longer make grammatical sense. Accordingly, we affirm the district court's severability analysis insofar as it enjoined these provisions on the basis that they are not severable from the DPIA report requirement.

However, we vacate the district court's determination that the DPIA report requirement is unlikely to be functionally severable from the remainder of the law. For instance, NetChoice has failed to show why the CAADCA's "Children's Data Protection Working Group," which is tasked with making recommendations to the California State Legislature on "best practices" concerning the data privacy of children, cannot function without the DPIA report requirement. *See id.* § 1798.99.32. The working group can certainly "stand on [its] own," with or without the DPIA report requirement. *People's Advoc.*, 226 Cal. Rptr. at 649. It is capable of "separate enforcement." *Id.*

We also think it is a much closer question than the district court assumed whether the elimination of the 90-day cure period, which cannot operate without the DPIA report requirement, *see* Cal. Civ. Code § 1798.99.35(c), necessarily dooms the Attorney General's civil enforcement of other provisions of the CAADCA. The district court likened the 90-day cure period as a "condition precedent" to enforcing other provisions in the CAADCA, but that is not necessarily true. As the State persuasively argues, a business can functionally comply with, for instance, the unchallenged requirement that it "provide an obvious signal to child users when they are being tracked," *id.* § 1798.99.31(a)(8), even if the business did not complete a DPIA report and even if no cure period is available. However, we cannot discern at this stage of the litigation if elimination of the 90-day cure period affects whether provisions concerning the Attorney General's civil enforcement of valid sections of the CAADCA are volitionally severable.

CONCLUSION

For the foregoing reasons, we **AFFIRM** the district court's preliminary injunction insofar as it enjoined enforcement of California Civil Code §§ 1798.99.31(a)(1)–(4), (c), 1798.99.33, 1798.99.35(c), and **VACATE** the remainder of the preliminary injunction.[9] Both parties shall bear their own costs on appeal. *See* Fed. R. App. P. 39(a)(4).

All Citations

--- F.4th ----, 2024 WL 3838423

Footnotes

1 Unless the CAADCA provides an alternative definition for a term, it expressly incorporates the definitions provided in the CCPA. *Id.* § 1798.99.30(a). The CAADCA defines "likely to be accessed by children" to mean "it is reasonable to expect, based on [enumerated] indicators, that the online service, product, or feature would be accessed by children." *Id.* § 1798.99.30(b)(4). The enumerated indicators include whether the online service "is directed to children," *id.* § 1798.99.30(b)(4)(A), whether it is "routinely accessed by a significant number of children," *id.* § 1798.99.30(b)(4)(B), and

whether it "has design elements that are known to be of interest to children, including, but not limited to, games, cartoons, music, and celebrities who appeal to children," *id.* § 1798.99.30(b)(4)(E).

2 The CAADCA defines "profiling" as "any form of automated processing of personal information that uses personal information to evaluate certain aspects relating to a natural person, including analyzing or predicting aspects concerning a natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements." Cal. Civ. Code § 1798.99.30(b)(6).

3 The district court cited the Eleventh Circuit's decision in *NetChoice, LLC v. Attorney General, Florida*, for the following proposition: "When platforms choose to remove users or posts, deprioritize content in viewers' feeds or search results, or sanction breaches of their community standards, they engage in First-Amendment-protected activity." *NetChoice*, 692 F. Supp. 3d at 945 (quoting *NetChoice, LLC v. Atty. Gen., Fla.*, 34 F.4th 1196, 1213 (11th Cir. 2022)). The Supreme Court recently vacated the decision, but largely affirmed that principle of law. *See Moody v. NetChoice, LLC*, —— U.S. ——, 144 S. Ct. 2383, 2394, 2399–2400, —— L.Ed.2d —— (2024).

4 The district court referred to the intermediate scrutiny standard set forth in *Central Hudson Gas & Electric Corporation v. Public Service Commission of New York*, 447 U.S. 557, 100 S.Ct. 2343, 65 L.Ed.2d 341 (1980), as "commercial speech scrutiny." *NetChoice*, 692 F. Supp. 3d at 941 n.3.

5 NetChoice's complaint did not specifically challenge § 1798.99.31(b)(2), which regulates child profiling. Nonetheless, NetChoice challenged it as a content-based restriction in its motion for a preliminary injunction, and the district court discussed it specifically in its order. *NetChoice*, 692 F. Supp. 3d at 955–56.

6 The district court suggested that it did not consider NetChoice's overbreadth challenges. *NetChoice*, 692 F. Supp. 3d at 939–40. However, the test described here applies to both First Amendment facial challenges and overbreadth challenges. *Compare Moody*, 144 S. Ct. at 2397 (discussing the proper standard for a facial challenge), *with United States v. Hansen*, 599 U.S. 762, 769, 143 S.Ct. 1932, 216 L.Ed.2d 692 (2023) (discussing the rules for an overbreadth challenge).

7 Because most of the required factors relate to compelled speech about potential content-related harms to children, we do not reach whether a more limited DPIA report requirement for businesses to consider whether a product "uses system design features to increase, sustain, or extend use of" a product by children, Cal. Civ. Code § 1798.99.31(a)(1)(B)(vii), or whether a product "collects or processes sensitive personal information of children," *id.* § 1798.99.31(a)(1)(B)(viii), would survive First Amendment scrutiny.

8 According to Amici Design Scholars, examples of dark patterns may include the "infinite scroll" feature on X (formerly Twitter), "autoplay" on YouTube and TikTok, and "streaks" on Snapchat.

9 The panel need not reach any of the alternative grounds for affirming the district court's preliminary injunction. Those issues are inadequately briefed on appeal, and the district court has not meaningfully evaluated the parties' arguments in the first instance. *See generally Detrich v. Ryan*, 740 F.3d 1237, 1248–49 (9th Cir. 2013) (en banc) (observing that it is "standard practice ... to remand to the district court for a decision in the first instance without requiring any special justification for so doing"), *overruled on other grounds by Shinn v. Ramirez*, 596 U.S. 366, 142 S.Ct. 1718, 212 L.Ed.2d 713 (2022); *Ecological Rts. Found. v. Pac. Lumber Co.*, 230 F.3d 1141, 1154 (9th Cir. 2000) (discussing prudential reasons why an appellate court typically does not address alternative grounds for affirmance).

End of Document